INTERCONNECTION SECURITY AGREEMENT

June, 2006

U. S. Department of Homeland Security

Customs and Border Protection

INTERCONNECTION SECURITY AGREEMENT

The intent of the Interconnection Security Agreement (ISA) is to document and formalize the interconnection agreement between Customs and other non-Customs organizations.

1. INTERCONNECTION STATEMENT OF REQUIREMENTS.

a. The requirements for interconnection between the Customs and Border Protection (CBP) and your company is for the express purpose of the following:

- Provide your company with VPN tunnel connectivity to CBP for the purpose of allowing your company to send/receive data, to/from CBP, via MQ Client/Server.

b. No other services are authorized under this agreement. Other than the passing of data stated in paragraph 1a, only communication control signals typical of Transmission Control Protocol/Internet Protocol (TCP/IP) and MQ Client/Server will be permitted.

c. Data transmitted between your designated end-point system and CBP will be protected (encrypted) in accordance with the guidelines of the Privacy Act, Trade Secrets Act (18 U. S. Code 1905), and Unauthorized Access Act (18 U. S. Code 2701 & 2710). Transaction data returned to your system remains protected (encrypted) until transmitted through the layer-3 VPN tunnel connected to your system, at which point the data is decrypted (open and unprotected) for final transmission into your system. Your company is responsible for providing any further protection measures for your company data when resident in your computing environment, as necessary.

2. SYSTEM SECURITY CONSIDERATIONS.

a. The interconnection between your company and CBP is via the public Internet, over a Triple Data Encryption System (3DES) protected VPN tunnel. Authentication will be via CBP provided user ID and password and/or pre-share keys.

b. The security of the information being passed on this layer-3 VPN connection uses either Cisco VPN hardware or software.

c. The CBP system and users are expected to protect this data in accordance with the Privacy Act, Trade Secrets Act (18 U.S. Code 1905), and Unauthorized Access Act (18 U.S. Code 2701 & 2710).

d. The sensitivity of all data filed is Sensitive But Unclassified (SBU).

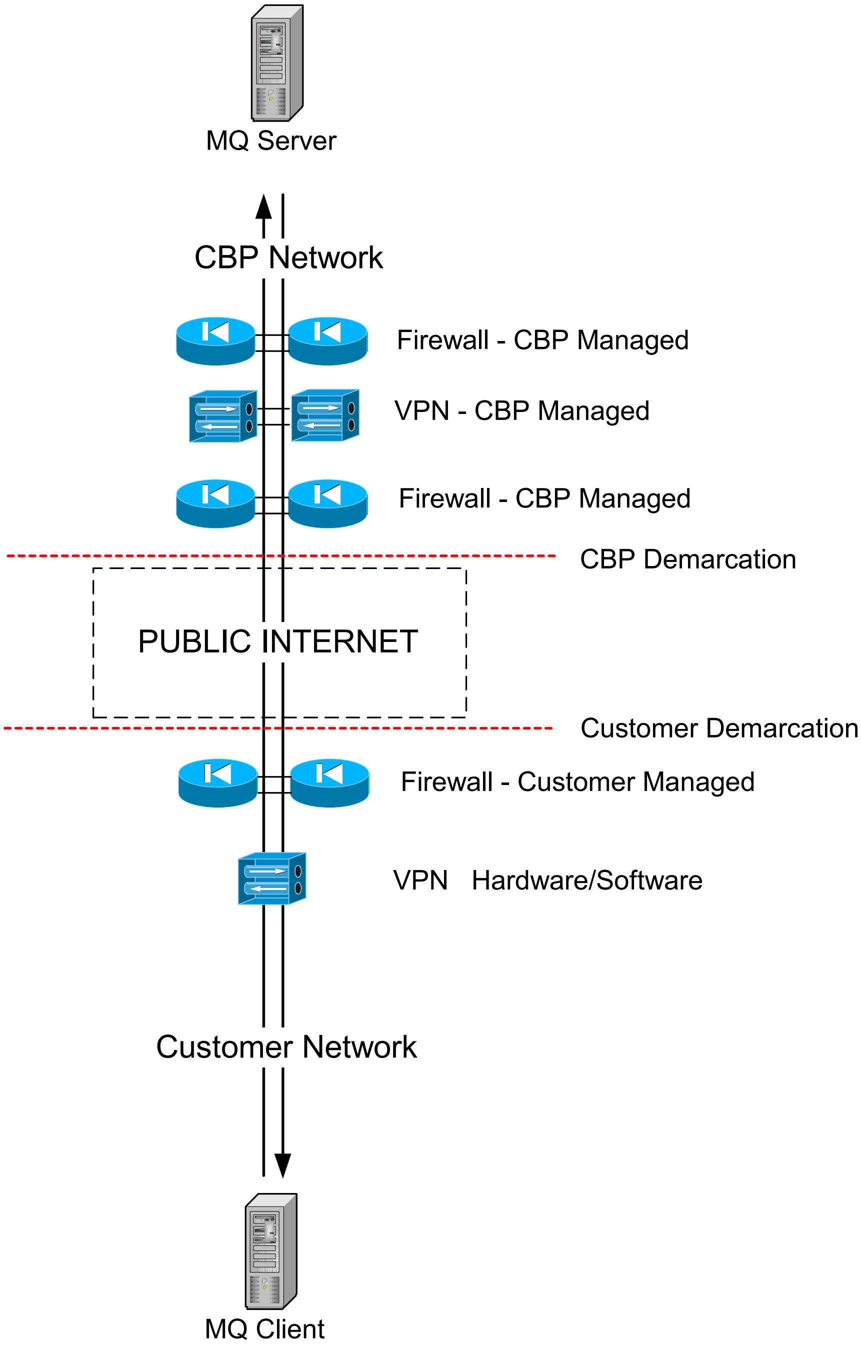
e. All CBP employees with access to the data are U. S. citizens with a valid and current CBP Background Investigation.

f. Policy documents that govern the protection of the data are CBP (Customs) CIS HB 1400-05B and Department of Homeland (DHS) –4300A Sensitive Systems Policy.

g. CBP maintains an audit trail and employs intrusion detection measures to maintain security and system integrity.

h. All security incidents that have any effect on the security posture of CBP must be reported to the CBP Computer Security Incident Response Center (CSIRC) located at the CBP NDC (tel: 703-921-6507). The policy governing the reporting of security incidents is CIS HB 1400-05B.

3. TOPOLOGICAL DRAWING. The two systems are joined via a layer-3 IPSEC VPN tunnel. The CBP NDC facility maintains a 24-hour physically secure facility where access is controlled using restricted access and all visitors are escorted. The lines of demarcation are as illustrated in the following drawing:



4. **SIGNATORY AUTHORITY.** This ISA is valid upon electronic acknowledgement of receipt of an agreement from your designated corporate approval authority. The ISA will be reviewed, validated, stored and tracked for periodic renewal by CBP. This agreement may be terminated upon 30-days advanced notice by either party or in the event of a security exception that would necessitate an immediate response.

John R. MacDonald
Assistant Commissioner,
Office of Information & Technology
Customs and Border Protection